Internat. J. Math. & Math. Sci.
Vol. 4 No. 1 (1981) 101-107

RINGS AND GROUPS WITH COMMUTING POWERS

HAZAR ABU-KHUZAM
ADIL YAQUB

DEPARTMENT OF MATHEMATICS
PETROLEUM UNIVERSITY
SAUDI ARABIA

(Received March 5, 1979)

ABSTRACT. Let n be a fixed positive integer. Let R be a ring with identity which satisfies (i) $x^n y^n = y^n x^n$ for all x, y in R, and (ii) for x, y in R, there exists a positive integer $k = k(x,y)$ depending on x and y such that $x^k y^k = y^k x^k$ and $(n,k) = 1$. Then R is commutative. This result also holds for a group G. It is further shown that R and G need not be commutative if any of the above conditions is dropped.

KEY WORDS AND PHRASES. ring, group, center, Jacobson radical, commutative.

1980 *MATHEMATICS SUBJECT CLASSIFICATION CODES: Primary* 16A70, 20F10; *Secondary* 16A38.

1. INTRODUCTION.

Throughout this section, n is a fixed positive integer. The main theorem of this section is the following:

THEOREM 1. *Let* G *be a group such that* (i) $x^n y^n = y^n x^n$ *for all* x, y *in* G, *and* (ii) *for* x, y *in* G, *there exists a positive integer* $k = k(x,y)$,

depending on x *and* y *such that* $x^k y^k = y^k x^k$ *and* $(n,k) = 1$. *Then* G *is commutative*.

In preparation for the proof of Theorem 1, we first prove the following Lemma.

LEMMA 1. *Let* G *be as in Theorem* 1. *Then for every finite subset* F *of* G, *there exists a positive integer* $N = N(F)$, *depending on* F *such that* $x^N y^N = y^N x^N$, *and* $x^{N+1} y^{N+1} = y^{N+1} x^{N+1}$ *for all* x, y *in* F.

PROOF. Let x_1, y_1, x_2, and $y_2 \in G$. Then by condition (ii) above there exist positive integers $k_1 = k_1(x_1,y_1)$, $k_2 = k_2(x_2,y_2)$, both relatively prime to n, such that

$$x_1^{k_1} y_1^{k_1} = y_1^{k_1} x_1^{k_1} \text{ and } x_2^{k_2} y_2^{k_2} = y_2^{k_2} x_2^{k_2} .$$

Let $k = k_1 k_2$. Then, clearly k is relatively prime to n, and

$$x_1^k y_1^k = y_1^k x_1^k, \quad x_2^k y_2^k = y_2^k x_2^k.$$

It follows easily, that for any finite subset F of G there exists a positive integer $k = k(F)$ which is relatively prime to n and, $x^k y^k = y^k x^k$ for all x, y in F. From (i) we know that $x^n y^n = y^n x^n$ for all x, y in G. Since k and n are relatively prime, $rk - sn = 1$ for some positive integers r and s. If $N = sn$ then $N + 1 = rk$ and it follows that $x^N y^N = y^N x^N$, $x^{N+1} y^{N+1} = y^{N+1} x^{N+1}$, for all x, y in F. Clearly, N depends on F. This proves Lemma 1.

PROOF OF THEOREM 1. Let x, y $\in$ G, and let $F = \{x,y,xy,yx\}$. Then by Lemma 1 there exists a positive integer $N = N(F)$ such that $a^N b^N = b^N a^N$ and $a^{N+1} b^{N+1} = b^{N+1} a^{N+1}$ for all a, b in F. Also, x, y $\in$ F implies $x^N y^N = y^N x^N$ and $x^{N+1} y^{N+1} = y^{N+1} x^{N+1}$. Hence $x^N = y^{-N} x^N y^N$ and $x^{N+1} = y^{-(N+1)} x^{N+1} y^{N+1}$. Now $x = x^{N+1} \cdot x^{-N} = y^{-(N+1)} x^{N+1} y^{N+1} y^{-N} x^{-N} y^N$, and hence

$$x = y^{-(N+1)} x^{N+1} y x^{-N} y^N. \tag{1}$$

Multiplying equation (1) by y from the right we get

$$xy = y^{-(N+1)} x^{N+1} y x^{-N} y^{N+1}$$

and thus

$$(xy) = y^{-(N+1)}x^{N+1}(yx)x^{-(N+1)}y^{N+1}$$

Raising both of the above equation to the power (N+1) we get

$$(xy)^{N+1} = y^{-(N+1)}x^{(N+1)}(yx)^{N+1}x^{-(N+1)}y^{N+1}.$$

Hence $(xy)^{N+1} = (yx)^{N+1}$, since x, y and yx ε F. Multipling equation (1) by y from the left we get

$$yx = y^{-N}x^{N+1}yx^{-N}y^{N},$$

and hence

$$yx = y^{-N}x^{N}(xy)x^{-N}y^{N}.$$

Raising both sides of the above equation to the power N we get

$$(yx)^{N} = y^{-N}x^{N}(xy)^{N}x^{-N}y^{N}.$$

But since x, y, xy ε F we get

$$(yx)^{N} = (xy)^{N}.$$

Now $(xy) = (xy)^{N+1} \cdot (xy)^{-N} = (yx)^{N+1} \cdot (yx)^{-N} = yx$, and hence G is abelian

2. RINGS.

Throughout this section, R is an associative ring with identity 1 and $[x,y] = xy - yx$ for x, y in R.

In preparation for the proof of the main theorem of this section, we first prove the following:

LEMMA 2. *Suppose* x *and* y *are elements of* R, *satisfying* $kx^{m}[x,y] = 0$ *and* $k(x+1)^{m}[x,y] = 0$, *for some positive integers* k *and* m. *Then* $k[x,y] = 0$.

PROOF. Expanding $(x+1)^{m}$ in $k(x+1)^{m}[x,y] = 0$ we get

$$kx^{m}[x,y] + kc_{m-1}x^{m-1}[x,y] + \ldots + kc_{1}x[x,y] + k[x,y] = 0. \quad (2)$$

By hypothesis, $kx^{m}[x,y] = 0$, so if m = 1 then the result follows immediately from (2). Suppose m > 1. Now, multiply equation (2) by x^{m-1} from the left, and use the hypothesis $kx^{m}[x,y] = 0$ to get $kx^{m-1}[x,y] = 0$. Equation (2) becomes:

$$kc_{m-2}x^{m-2}[x,y] + \ldots + kc_{1}x[x,y] + k[x,y] = 0. \quad (3)$$

If $m = 2$, then since $kx^{m-1}[x,y] = 0$, the result follows immediately from (2) Suppose $m > 2$. Now, multiplying equation (3) by x^{m-2} from the left, and use the fact that $kx^{m-1}[x,y] = 0$ to get $kx^{m-2}[x,y] = 0$. Continue this process until we get $k[x,y] = 0$, which proves the lemma.

Now we will prove the analogue to Theorem 1 for rings.

THEOREM 2. *Let n be a fixed positive integer. Suppose that R is an associative ring with identity 1 such that (i) $x^n y^n = y^n x^n$ for all x, y in R, and (ii) for x, y in R, there exists a positive integer $k = k(x,y)$, depending on x and y which is relatively prime to n such that $x^k y^k = y^k x^k$. Then R is commutative.*

In preparation for the proof of Theorem 2, we first state the following lemma.

LEMMA 3. *Let R be as in Theorem 2. Then for every finite subset F of R, there exists a positive integer $N = N(F)$, depending on F such that $x^N y^N = y^N x^N$ and $x^{N+1} y^{N+1} = y^{N+1} x^{N+1}$ for all x, y in F.*

PROOF. Exactly the same as the proof of Lemma 1.

PROOF OF THEOREM 2. Throughout the proof, J, Z and R^* will denote respectively the Jacobson radical, the center, and the group of units of R. The proof is broken into the following partial results.

CLAIM 1. R^* is abelian, and R/J is commutative.

PROOF. R^* is abelian, by Theorem 1. It is easy to see that the above hypotheses are inherited by subrings and by homomorphic images of R. Also, the above hypotheses imply that the idempotents are in the center, and hence no $m \times m$ complete matrix ring over a division ring can satisfy our hypotheses for $m > 1$. So by the Jacobson Density Theorem, a primitive ring satisfying our hypotheses must be a division ring, and hence is commutative, by Theorem 1. Also, R/J is semisimple, and hence it is a subdirect sum of primitive rings.

So R/J is commutative.

CLAIM 2. J is commutative, and $J^2 \subseteq Z$.

PROOF. Suppose a, b ε J. Then a + 1 belong to R^*, and hence they commute by Claim 1. So ab = ba, and J is commutative. For x ε R, we have

$$(ab)x = a(bx) = (bx)a = b(xa) = (xa)b = x(ab).$$

So ab ε Z, and hence $J^2 \subseteq Z$.

For the remainder of this proof, let a ε J, y ε R. Let $F' = \{a,y,a+1,y+a, y+1\}$. Then by Lemma 3, there exists a positive integer $N = N(F')$ such that $c^N d^N = d^N c^N$ and $c^{N+1}d^{N+1} = d^{N+1}c^{N+1}$ for all c, d ε F′.

CLAIM 3. $N[a,y^N] = 0 = (N+1)[a,y^{N+1}]$.

PROOF. Since a ε J, u = 1 + a ε R^*. Also, R/J is commutative, and hence $[u,y^N] \varepsilon J$. So u commutes with $[u,y^N]$, and hence by induction, $0 = [u^N,y^N] = Nu^{N-1}[u,y^N]$. This implies that $N[u,y^N] = 0$, since u is invertible. Hence $N[a,y^N] = 0$. Similarly, since $[u^{N+1},y^{N+1}] = 0$, we have $(N+1)[a,y^{N+1}] = 0$.

CLAIM 4. $N[a,y] = 0$ and $[a,y^{N+1}] = 0$.

PROOF. Since y ε F′ and y + a ε F′, we have

$$[(y+a)^{N+1},y^{N+1}] = 0.$$

Since a ε J, $a^2 \varepsilon Z$, and hence the only terms in the expansion of $(y+a)^{N+1}$ which do not commute with y^{N+1} are those involving one a. So

$$0= [(y+a)^{N+1},y^{N+1}] = [y^N a + y^{N-1}ay + \dots + yay^{N-1} + ay^N,y^{N+1}]. \quad (4)$$

By Claim 3, $Ny^N a = Nay^N$, and so we can write the following:

$$N(y^N a + y^{N-1}ay + \dots + yay^{N-1} + ay^N)y^{N+1}$$

$$=N(y^{2N}ay + y^{2N-1}ay^2 + \dots + y^{N+1}ay^N) + Nay^{2N+1},$$

and

$$Ny^{N+1}(y^N a + y^{N-1}ay + \ldots + yay^{N-1} + ay^N)$$

$$= Ny^{2N+1}a + N(y^{2N}ay + \ldots + y^{N+1}ay^N).$$

By (4), the expressions on the left of the above two equations are equal, and hence we have $Nay^{2N+1} = Ny^{2N+1}a$. But $Ny^{2N}a = Nay^{2N}$, by Claim 3. So $Ny^{2N}[y,a] = 0$. Now, since $y + 1 \in F'$, the same result holds for $(y + 1)$ instead of y. So $N(y + 1)^{2N}[y,a] = 0$, and hence by Lemma 2, we have $N[y,a] = 0$. By Claim 3, $(N+1)[a,y^{N+1}] = 0$, and hence $N[a,y^{N+1}] + [a,y^{N+1}] = 0$. But $N[a,y^{N+1}] = 0$, since $N[a,y^N] = 0$ and $N[a,y] = 0$. Therefore, $[a,y^{N+1}] = 0$.

Now we can complete the proof of Theorem 2. Since $y + a$ and y belong to F', $[(y + a)^N, y^N] = 0$. Also, $a^2 \in Z$. Hence,

$$[y^{N-1}a + y^{N-2}ay + \ldots + yay^{N-2} + ay^{N-1}, y^N] = 0. \qquad (5)$$

By Claim 4, $ay^{N+1} = y^{N+1}a$, and hence we can write the following:

$$(y^{N-1}a + y^{N-2}ay + \ldots + yay^{N-2} + ay^{N-1})y^N$$

$$= y^{N-1}ay^N + (y^{2N-1}a + y^{2N-2}ay + \ldots + y^{N+1}ay^{N-2}),$$

and

$$y^N(y^{N-1}a + y^{N-2}ay + \ldots + yay^{N-2} + ay^{N-1})$$

$$= (y^{2N-1}a + y^{2N-2}ay + \ldots + y^{N+1}ay^{N-2}) + y^N ay^{N-1}.$$

By (5), the above two expressions on the left are equal, and hence $y^{N-1}ay^N = y^N ay^{N-1}$. Multiply this equation from the left and right by y to get $y^N ay^{N+1} = y^{N+1}ay^N$. Then, using Claim 4, we get $y^{2N+1}a = ay^{2N+1}$. But from Claim 4, we have $ay^{2N+2} = y^{2N+2}a$. So $y^{2N+1}[a,y] = 0$. Now since $y + 1 \in F'$, the above result holds for $y + 1$, and hence $(y + 1)^{2N+1}[a,y] = 0$.

But then by Lemma 2, we have $[a,y] = 0$. This proves that $J \subseteq Z$. Now, let $x, y \in R$. Then $[x,y] \in J$, since R/J is commutative. Therefore, $[x,y] \in Z$, since $J \subseteq Z$. Let $F'' = \{x,y,x+1,y+1\}$. Then by Lemma 3, there exists a positive integer $k = k(F'')$ such that $c^k d^k = d^k c^k$ and $c^{k+1} d^{k+1} = d^{k+1} c^{k+1}$ for all $c, d \in F''$. Recall that $[x,y] \in Z$ and hence, by induction, we see that $0 = [x^k, y^k] = kx^{k-1}[x,y^k]$. Since $x + 1 \in F''$, the same result holds for $x + 1$ replacing x, and hence $k(x+1)^{k-1}[x,y^k] = 0$. Then, by Lemma 2 we have $k[x,y^k] = 0$. So, by induction as in above, $0 = k[x,y^k] = k^2 y^{k-1}[x,y]$. Again, since $y + 1 \in F''$, the same result holds for $y + 1$ replacing y, so $k^2(y+1)^{k-1}[x,y] = 0$. Applying Lemma 2, we get $k^2[x,y] = 0$. Similarly, since $[x^{k+1}, y^{k+1}] = 0$, we get $(k+1)^2 [x,y] = 0$, and hence $[x,y] = 0$ which proves Theorem 2.

We conclude with the following remarks:

REMARK 1. A finite nonabelian group shows that we cannot drop any of the hypotheses in Theorem 1.

REMARK 2. Theorem 2 need not be true if R has no identity. For, let R be a finite nil non-commutative ring.

REMARK 3. Theorem 2 need not be true if either condition (i) or (ii) is deleted. For, let

$$R = \begin{pmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{pmatrix} : a,b,c,d \in GF(2) .$$

Then $x^2 y^2 = y^2 x^2$ for all $x, y \in R$.

Related work appears in [1] and [2].

REFERENCES

[1] Bell, H.E., On Rings with Commuting Powers, Math. Japonica 24(1979), 473-478.

[2] Hongan M and Tominaga H., A Commutativity Theorem for S-Unital Rings, Math. J. Okayama Univ. 21(1979), 11-14.

[3] Nicholson W.K. and Yaqub A., A Commutativity Theorem for Rings and Groups, Canadian Mathematical Bulletin 22(1979), 419-423.